Planul de Securitate a Sistemelor Informatice şi de Comunicaţii

Introducere

Regulamentele de utilizare a Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în Spitalul de Psihiatrie Cavnic. (denumit pe scurt SPDPC)

Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii SPDPC în ansamblu și in particular a personalului contractual și al pacienților.

Scop

În acord cu legislaţia în vigoare din România, Regulamentele de Ordine Interioară ale Spitalul de psihiatrie Cavnic, resursele informatice şi de comunicaţii sunt Valori care trebuie exploatate **exclusiv** în folosul SPDPC . Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii actului medical.
- Protejarea datelor confidențiale generate în cadrul activității medicale a SPDPC.
- Respectarea normelor GDPR.
- Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate ori transportate folosind resursele informatice şi de comunicaţii ale utilizatorilor autorizaţi: cadre medicale, personal administrativ, colaboratori care au obținut dreptul de a accesa sistemele informatice, etc.
- Educarea utilizatorilor resurselor informatice şi de comunicaţii în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora.
- Compatibilitate cu legile, regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Adresabilitate

Regulamentele de utilizare a resurselor informatice şi de comunicaţii ale Spitalului de Psihiatrie Cavnic se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

Proceduri de elaborare, modificare şi aprobare a Regulamentelor

- Regulamentele de utilizare a Resurselor Informatice şi de Comunicaţii ale SPDPC se elaborează unitar și se aplică tuturor secțiilor și departamentelor.
- Regulamentele vor fi elaborate de către manager şi vor fi propuse pentru aprobare comitetului director și consiliului de administrație al Spitalului de Psihiatrie Cavnic.
- Prevederile Politicii de Securitate aprobate vor fi incluse în contractul de muncă şi toate contractele cu terţi (dacă activitatea acestora are legătură cu sistemul informatic şi de comunicaţii al SPDPC).
- Regulamentele de utilizare a sistemului resurselor informatice şi de comunicaţii vor fi

disponibile și în format electronic pe site-ul Spitalului de psihiatrie Cavnic la adresa web **https://www.spitalpsihiatriecavnic.ro/regulamente.html.**

- Prezentul document conţine o listă a tuturor regulamentelor aplicabile în sistemul resurselor Informatice şi de Comunicaţii.

Lista regulamentelor aplicabile, proceduri şi regulamente specifice

- Accesul la un sistem informatic se face exclusiv pe baza de parolă stabilită individual și care va fi cunoscută doar de persoana care folosește acel sistem informatic.
- Protejarea datelor conținute în fiecare sistem informatic precum și în rețeaua informatică a SPDPC este responsabilitatea fiecărui angajat facând parte din personal medical și administrativ.
- Respectarea normelor GDPR este obligatorie de către fiecare operator a unui sistem informatic aflat in rețeaua SPDPC.
- Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate ori transportate folosind resursele informatice şi de comunicaţii ale utilizatorilor autorizaţi: cadre medicale, personal administrativ, colaboratori care au obținut dreptul de a accesa sistemele informatice.
- Accesul persoanelor neautorizate la sistemele informatice ale SPDPC este interzis.
- Utilizatorii trebuie să anunţe conducerea în cazul în care se observă orice problemă/breşă în sistemul de securitate SPDPC cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
- Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip

- Utilizatorii nu trebuie să încerce să obţină acces la date sau programe pentru care nu au autorizaţie sau consimţământ explicit.
  - Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.
- Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
  - Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele reţelei informatice; să împiedice accesul unui utilizator autorizat; să obţină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente.
- Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii reţelei informatice. De exemplu, utilizatorii nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.
- Resursele informatice şi de comunicaţii ale SPDPC nu trebuie folosite pentru beneficiul personal.
- Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care SPDPC le poate considera ofensive, indecente sau obscene.
- Accesul rețelelor de socializare (facebook, tik-tok, instagram, telegram, discord, whatsup, etc) de pe sistemele informatice ale SPDPC în timpul programului de lucru este interzis.
- Accesul la reţeaua internet prin intermediul resurselor informatice şi de comunicaţii ale SPDPC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la aceste resurse.

- Utilizatorii care au acces la sistemele informatice al SPDPC au obligaţia de a purta ecusonul de identificare care să ateste calitatea de angajat, autorizat să acceseze resursele informatice și de comunicații.
- Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor și misiunii SPDPC.
- Accesul fizic al oricărui colaborator sau terț în încăperea unde se află serverele se face numai insoțit de persoana responsabilă de rețeaua IT, angajată a SPDPC și se notează în registrul de acces fizic.
- Introducerea stick-urilor usb, hard-disk-urilor externe ori a altor dispozitive în oricare dintre servere este interzisă.
- Nerespectarea regulilor de mai sus cât și adăugarea de dispozitive electronice, hardware sau software în rețeaua informatică și de comunicaţii a SPDPC fără drept și sau fără aprobare scrisă se considera o incălcare a Legii 286/2009 art 360 aliniatele 1,2,3 și anume:
- (1) Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.
- (2) Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.
- (3) Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

Utilizarea Ocazională

- În anumite situaţii este permisă utilizarea ocazională a sistemelor informatice. În aceste situaţii se aplică următoarele restricţii:
- Utilizarea personală ocazională a serviciilor de poştă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.
- Utilizarea ocazională a sistemelor informatice nu trebuie să aibă drept rezultate costuri directe pentru SPDPC.
- Utilizarea ocazională a sistemelor informatice nu trebuie să afecteze activitatea normală a angajaţilor.
- Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva SPDPC sau prejudicierea, indiferent de formă, a intereselor Spitalului de psihiatrie Cavnic.
- Nu se vor divulga parolele wi-fi pentru utilizare ocazională.

Regulament privind Accesul Fizic la Sistemele Informatice și de Comunicații

- Toate sistemele de securitate fizică (de exemplu coduri de acces în clădire şi coduri de acces pentru prevenirea incendiilor etc.) trebuie să fie instalate în conformitate cu regulamentele SPDPC.
- Accesul fizic la toate încăperile în care sunt instalate servere trebuie să fie documentat şi monitorizat.
- Toate încăperile în care sunt instalate servere trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
- Pentru fiecare încăpere în care sunt instalate echipamentele de rețea ale sistemului informatic se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi dacă este cazul, părţilor contractante, ale căror obligaţii contractuale

implică acces fizic.

- Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
- Acordarea drepturilor de acces (folosind card-uri, chei, parole etc.) se face în scris de către conducerea SPDPC sau, după caz, persoana responsabilă care deţine încăperea şi resursele.
  - Nu este permis transferul dreptului de acces indiferent de motiv.
- Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate la secretariatul SPDPC.
  - Accesul restricţionat trebuie marcat.
- Pentru fiecare spaţiu cu acces restricţionat trebuie desemnată o persoană care să verifice .

Regulament de Tratare a Incidentelor de Securitate

- Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.
  - Angajatul este responsabil cu înştiinţarea conducerii despre incident.
- Persoana desemnată cu administrarea reţelei IT este responsabilă cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.
- Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.
- Administratorul IT va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.
- Administratorul IT trebuie să comunice conducerii SPDPC nivelul resurselor afectate de incident, informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.
  - Administratorul IT este responsabil cu documentarea anchetei privind incidentul.
- Administratorul IT este responsabil de coordonarea activităţilor de comunicare cu terţi autorizaţi pentru rezolvarea incidentului.
- În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare Administratorul IT va recomanda SPDPC un plan de acţiune.
  - În cazul în care incidentul implică aplicarea legilor civile sau penale managerul SPDPC va recomanda sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

Regulament de Monitorizare Sistemelor Informatice

- Monitorizarea resurselor informatice şi de comunicaţii ale SPDPC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:
  - Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
  - Tipul traficului în reţeaua, a protocoalelor şi a echipamentelor conectate, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
  - Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

- Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale SPDPC. În această categorie intră următoarele (fără a se limita doar la acestea):

- Jurnale ale sistemelor de detectarea automată a intruşilor;
- Jurnale Firewall;
- Jurnale ale activităţii conturilor utilizator;
- Jurnale ale scanărilor reţea;
- Jurnale ale aplicaţiilor;
- Jurnale ale solicitărilor de suport tehnic;
- Jurnale ale erorilor din sisteme şi servere.

- În mod regulat (cel puţin o dată la şase luni) se vor efectua verificări, de către persoana desemnata din cadrul SPDPC pentru detectarea:
  - Parolelor utilizator care nu respectă regulamentele;
  - Echipamentelor de reţea conectate neautorizat;
  - Serviciilor de reţea neautorizate;
  - Serverelor de pagini de web neautorizate;
  - Echipamentelor ce utilizează resurse comune nesecurizate;
  - Utilizării de echipamente neautorizate;
  - Licenţelor pentru sistemele de operare şi programele instalate.
- Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către managementul SPDPC în scopul efectuării de investigaţii.
- Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:
  - Instalarea sistemului de operare dintr-o sursă aprobată; Licență.
  - Aplicarea patch-urilor furnizate de producător, furnizorul software
- Înlăturarea programelor, a serviciilor sistem şi a driver-lor care nu sunt necesare;
- Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
  - Dezactivarea sau schimbarea parolelor conturilor predefinite;
  - Securizarea accesului fizic la aceste echipamente.
- Administratorul IT va monitoriza obligatoriu pentru serverele principale (enterprise) procesul de instalare şi aplicare regulată a patch-urilor de securitate şi, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

Regulament privind Crearea şi Utilizarea Copiilor de Siguranţă (Backup)

- Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de departamentul care a creat datele, copiile de siguranța se fac periodic (zilnic, săptămânal. lunar sau anual după cum stabilește SPDPC).
- Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul SPDPC trebuie să fie documentată şi periodic revizuită.

- Furnizorul care oferă servicii de stocare a copiilor de siguranţă în alte zone pentru SPDPC trebuie să fie acreditat în acest scop de către o autoritate a statului.
- Procedurile stabilite între SPDPC şi furnizorii de stocare a copiilor de siguranţă în altă zonă trebuie să fie revizuite cel puţin anual.
- Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic.
- Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.
- Accesul la mediile de backup ale SPDPC stocate la furnizori externi sau în interior se va face folosind proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.
- Mediile utilizate pentru stocarea copiilor de siguranţă trebuie să aibă un sistem de identificare care să conţină cel puţin următoarele date de identificare a informaţiei stocate:
    - numele sistemului;
    - data creării copiei;
    - tipul de copie (completă, incrementală etc.);
    - clasificarea sensibilităţii (siguranţei/securităţii);
    - informaţii de contact.

Regulament pentru Detectarea Accesului Neautorizat

- Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).
- Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.
- Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.
- Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) de către administratorul IT.
- Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.
- Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.
- Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.
- Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.
- Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către conducerea SPDPC.
- Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile încălcări ale prezentul regulament.

Regulamentul privind Securitatea Informațiilor în cazul Calculatoarelor Portabile

- Calculatoarele portabile trebuie să fie protejate prin parole.
- Se va evita stocarea datelor care privesc SPDPC pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc SPDPC trebuie criptate utilizând tehnici aprobate de către managementul unității in colaborare cu administratorul IT.
- Transmiterea datelor prin reţele de tip wireless se poate face numai prin reţelele instalate de către SPDPC; acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise.
- Conectarea sistemelor de calcul care nu sunt proprietatea SPDPC se face numai cu aprobarea în scris a managerului.

Regulament pentru Modificări şi Modernizări ale Rețelei Informatice

- Orice modificare asupra unei componente de rețea din cadrul SPDPC, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.
- Toate modificările care afectează mediul de funcţionare a sistemelor componente ale rețelei informatice (ex: aparate de aer condiţionat, instalaţii de apă, încălzire, instalaţii electrice şi alarme) trebuie să fie anunţate şi aprobate în scris de către managementul SPDPC
- Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului informatic vor fi documentate şi aprobate de către conducerea SPDPC. Nu este permisă modificarea de către utilizatori, colaboratori sau terți a elementelor de infrastructură.
- Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea unității.
- Modificările planificate trebuie anunţate cu cel putin 48 ore înainte de a fi executate.
- Cererile de modificare planificată pot fi respinse în următoarele cazuri: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în mod negativ o activitate importantă a instituţiei sau resursele corespunzătoare necesare nu pot fi disponibile imediat.
- Se va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat sau nu cu succes.
- Trebuie întreţinută o bază de date care să cuprindă toate modificările. Aceasta trebuie să conţină cel puţin următoarele informaţii: data la care s-a făcut cererea pentru modificare şi data la care s-a făcut modificarea; informaţii de contact pentru utilizator; natura modificării; indicarea succesului sau nereuşitei modificării.

Regulament de Utilizare a reţelei Internet şi Intranet

- Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopul indeplinirii sarcinilor de serviciu in cadrul SPDPC.
- Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către conducere. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.
- Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.
- Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.
- Orice activitate a utilizatorilor folosind rețeaua informatică poate fi înregistrată şi ulterior examinată.
- Conţinutul tuturor site-urilor web ale SPDPC trebuie să se conformeze legilor în vigoare şi să folosească numele de domeniu al SPDPC (spitalpsihiatriecavnic.ro).
- Nu se vor publica pe site-urile web ale SPDPC materiale cu caracter ofensiv sau de hărţuire.
- Nu se vor publica pe site-urile web ale SPDPC materiale publicitare comerciale sau personale.
- Nu este permisă utilizarea rețelei informatice a SPDPC în scop personal sau pentru solicitări personale ce nu au legătură cu activitatea de serviciu.
- Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziţie ale SPDPC.
- Orice material confidenţial al SPDPC transmis prin reţeaua Internet trebuie criptat.
- Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentul regulament şi regulamentele proprii fiecărui secții sau departament

Regulament de Administrare a Conturilor

- Toate conturile create sunt valide pe perioada contractului de muncă.
- Toate conturile utilizator se vor crea în formatul Prenume.Nume.
- Prin contractul de muncă, contractul de colaborare şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului informatic.
- Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
- Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
- Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulamentul privind Parolele de Acces.
- Toate conturile utilizator care nu au fost accesate timp de 90 de zile vor fi dezactivate. După încă 90 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.
- SPDPC rebuie să aibă o documentaţie de modificare a conturilor utilizator pentru a se pune de acord în situaţii precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator.

Regulament pentru Parolele de Acces

- Toate parolele trebuie să îndeplinească următoarele condiţii:
    - Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 45 de zile;
    - Să aibă o lungime minimă de 8 caractere;
    - Să fie parole complexe;
    - Reutilizarea parolelor este interzisă;
    - Parolele stocate trebuie criptate;
- Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.
- Dispozitivele de securitate (ex. card Smart, semnătură electronică) trebuie returnate după terminarea relaţiilor cu SPDPC.
- Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
- Administratorul IT nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
- Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea SPDPC. Pentru ca o excepţie să fie aprobată, trebuie să existe o procedură pentru schimbarea parolelor.
- Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.
- Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:
- Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;
    - Se va genera o parolă care va fi comunicată utilizatorului;
- Utilizatorul va schimba parola temporară, comunicată anterior, în maxim 24 ore.

Regulament privind Sistemul de Mesagerie Electronică

- Următoarele activităţi sunt interzise de regulament:
    - Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
    - Folosirea sistemului de mesagerie electronică în scopuri personale;
- Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
- Următoarele activităţi sunt interzise deoarece împiedică buna funcţionare a comunicaţiilor în reţea şi eficienţa sistemelor de mesagerie electronică:
- Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
    - Trimiterea mesajelor de dimensiuni foarte mari;
    - Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.
- Toate informaţiile şi datele confidenţiale ale SPDPC, transmise către alte reţele externe, trebuie să fie criptate.
- Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea rețelei informatice ale SPDPC pot fi oricând înregistrate şi analizate.
- Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele SPDPC cu excepţia situaţiilor în care aceştia sunt

autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă SPDPC. Un exemplu de declaraţie simplă este: "părerile exprimate sunt personale, şi nu ale Spitalului de psihiatrie Cavnic … ".

- Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc SPDPC, folosind dispozitive de comunicaţii mobile care nu sunt autorizate de SPDPC. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenţi digitali personali,tablete, pagere ce permit trimiterea/primirea de informaţii şi telefoanele mobile/smartphone-uri.

Regulament de Detectare a Viruşilor

- Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a SPDPC, trebuie să utilizeze programe antivirus aprobate de către conducerea unității.
- Programele antivirus nu trebuie dezactivate.
- Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
- Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.
- Orice server de fişiere conectat la reţeaua Instituţiei trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.
- Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program.
- Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat conducerii unității.

Regulament de Relaţii cu Terţi

- Orice activitate desfăşurată de un furnizor care implică acces la rețeaua informatică trebuie să se conformeze cu regulamentele în vigoare ale SPDPC, cu procedurile standard şi convenţiile care cuprind, dar nu se limitează la următoarele:
    - Regulamente de Securitate a Accesului Fizic;
    - Regulamente de Confidenţialitate;
    - Regulamente de Securitate a Accesului la rețeaua informatică;
    - Regulamente de Modificare şi Modernizare;
    - Regulament de Utilizare Acceptabilă.
- În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:
    - Informaţiile din cadrul SPDPC, la care Furnizorul are drept de acces;
    - Modul în care informaţiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum şi măsuri ce vor fi luate în cazul nerespectării clauzelor;
    - Metodele de predare, distrugere sau de transfer al drepturilor informaţiilor SPDPC aflate în posesia Furnizorului, la încheierea contractului.
- Furnizorul trebuie să folosească sistemele informatice din cadrul SPDPC numai în scopul stipulat în contract.
- Orice altă informaţie din sistemul informatic al SPDPC obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.
- Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a SPDPC şi care

se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la rețea ale SPDPC, vor fi scoase din uz la încheierea relaţiilor contractuale.

- Accesul Furnizorului trebuie să fie identificat în mod unic, iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu Regulamentul privind Parolele de Acces ale SPDPC şi Regulamentul de Acces Administrativ.
- Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii SPDPC, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare.
- În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate SPDPC sau distruse în cel mult 24 de ore de la producerea evenimentului.
- În cazul terminării/rezilierii contractului sau la cererea SPDPC, Furnizorul va preda sau distruge toate informaţiile ce aparţin SPDPC şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.
- În cazul încheierii contractului sau la cererea SPDPC, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile SPDPC. Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuie documentate şi autorizate de Conducerea SPDPC .
- Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către SPDPC trebuie să fie inventariate corespunzător şi să posede drepturi de utilizare atestate prin Licenţe.

Orice încălcare a acestui regulament va fi adusă la cunoștința organelor în drept.
Acest regulament a fost prezentat tuturor angajaților spre cunoaștere și aplicare.

Manager
Mărginean Marius Doru